MARR GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E RESPONSABILIDADES

Julho de 2023

FOLHA DE CONTROLE

Informações Gerais

Título	Política de Segregação de Atividades e Responsabilidades
Elaborador	Ana Carolina Paifer
Data da Próxima Revisão	31/07/2024
Área Proprietária da Política	Compliance e Riscos Operacionais
Procedimentos e Outros Documentos Relacionados	Resolução CVM nº 21/2021; Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros

SUMÁRIO

1. INTRODUÇÃO

Nos termos da Instrução CVM nº 21 de 25/02/2021 em seu Artigo 27, bem como Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a Gestora, MARR Gestão de Recursos adota as regras e os procedimentos relativos à segregação de atividades de que possam gerar conflitos de interesse descritos no decorrer desta Política.

2. APLICABILIDADE

Esta Política é aplicável a todos os sócios, diretores parceiros e colaboradores, independentemente do nível hierárquico.

3. ATIVIDADES DESENVOLVIDAS

A MARR Gestão de Recursos ("MARR") atua exclusivamente na administração de carteiras de valores mobiliários, na categoria de Gestão de recursos de terceiros e na Distribuição de cotas dos fundos de investimento próprios, não prestando, portanto, quaisquer outros serviços no mercado de capitais.

4. SEGREGAÇÃO FÍSICA

Diante do supracitado, a MARR adota as seguintes regras:

O acesso de visitantes que não fazem parte do quadro de Colaboradores da MARR é restrito à recepção e às salas de reunião, exceto prévio conhecimento e autorização pela Administração da MARR, e desde que acompanhadas de Colaboradores da MARR, mediante identificação do visitante, com os registros através de foto e identificação de documentos. O atendimento aos clientes nas dependências da MARR deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

Não é permitida a circulação de Colaboradores em áreas que não sejam destinadas ao respectivo Colaborador.

Para as atividades de Gestão de recursos da MARR, existe uma área exclusiva, sendo a mesma, fisicamente segregada das demais áreas da Infinit. Inclusive, o acesso é restrito aos colaboradores integrantes da área, que somente podem acessá-la, por meio de crachás com controle eletrônico de acesso nas portas, visando garantir que não exista circulação de informações que possam gerar conflito de interesses.

Quanto às atividades relacionadas à distribuição de cotas dos fundos geridos, as mesmas também são totalmente segregadas das atividades de gestão, sendo seu acesso restrito aos colaboradores integrantes da área, por meio de crachás com controle eletrônico de acesso nas portas, visando garantir que não exista circulação de informações que possam gerar conflito de interesses.

O acesso às instalações é sempre controlado por meio com sistema de controle de acesso interno, que segrega o acesso a cada departamento, sempre identificando e registrando os acessos, com informações sobre o Colaborador, local, data e horário de acesso.

As áreas internas da MARR são totalmente segregadas, com acessos biométricos e câmeras de vigilância. A MARR possui procedimentos de chinese wall caso outras atividades venham a ser desenvolvidas, garantindo a total segregação em relação à atividade de gestão de carteiras, tanto nos espaços físicos como nos sistemas eletrônicos adotados.

Toda a Administração, Escrituração e Custódia dos fundos são realizadas por Instituições

Financeiras contratadas pelos mesmos para tais fins, de forma a evitar conflito de interesses nas atividades desenvolvidas.

No âmbito da prestação de serviços externos, os Colaboradores devem observar, ainda, as rotinas e procedimentos que tratam da confidencialidade das informações e sua segurança.

5. DEMAIS EQUIPES

Dentre as demais equipes designadas internamente pela MARR, destacam-se quatro equipes que são responsáveis pelo suporte das atividades prestadas pelas demais: tecnologia da informação, infraestrutura, expedição e serviços gerais.

As equipes de expedição e serviços gerais também prestam suporte às demais entidades do grupo da MARR. Vale ressaltar que o compartilhamento dessas equipes não configura um conflito de interesses, uma vez que se trata de serviços de suporte não relacionados diretamente às atividades principais desenvolvidas pela MARR de gestão de fundos de investimento.

Adicionalmente, os arquivos da rede possuem segregação por diretórios, de forma que os membros destas equipes não possuem acesso aos arquivos relacionados à atividade de gestão e demais práticas e controles internos da MARR.

Para maiores informações sobre as práticas, rotinas e procedimentos adotados em relação à segurança da informação, veja a Política de Segurança da Informação e Cibernética publicada na Intranet e Internet da MARR.

Quanto ao Compliance e a área de Riscos, ambas são segregadas das demais áreas da MARR, possuindo independência na execução de suas atividades, inclusive quanto aos acessos físicos e sistêmicos.

6. SEGREGAÇÃO ELETRÔNICA

A MARR segrega operacionalmente as atividades áreas a partir de equipamentos como: computador e telefone de uso exclusivo por cada colaborador, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não deve existir compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais colaboradores. Ainda, existe uma impressora destinada exclusivamente à utilização da área de administração de recursos.

A área de Segurança das informações conta com o bloqueio de portas USB e dos gravadores de mídia em todos os computadores, segregando as informações através de estrutura apartada de diretórios, onde cada Colaborador acessa somente às informações das respectivas equipes a que pertencem. O acesso se dá via login e senha individual a um diretório exclusivo, cujas informações e conteúdo disponível levam em consideração a atividade, nível hierárquico e departamento. Desta forma cada Colaborador só tem acesso aos sistemas e informações previamente autorizados pelos diretores da MARR.

Adicionalmente, o provedor de e-mail da MARR utilizado e a solução Microsoft Exchange Online, solução escalável e segura. Desta forma, todos os e-mails enviados pelo domínio da MARR seguem criptografados até o seu destinatário, evitando possíveis perdas ou furto de informações.

A senha de acesso é uma das ferramentas disponíveis para garantir a integridade e a confidencialidade dos dados da MARR, evitando eventual uso indevido. Para outros aplicativos adotados pela MARR, tais como os Sistemas DMA e Market Datas, dentre outros, a senha individual serve para garantir a disponibilidade do sistema a seu usuário legítimo e seu uso por um único Colaborador, evitando que a conexão em uso seja desconectada.

Para as medidas acima descritas sejam efetivas, é fundamental que a senha associada ao login individual seja criada pelo próprio Colaborador, com caracteres alfanuméricos e com no mínimo seis dígitos. Tal login e senha são de uso pessoal e intransferível, dando acesso exclusivo ao Colaborador aos sistemas da MARR. Este vínculo garante que o respectivo login seja utilizado somente por um único colaborador, não sendo possível a criação do mesmo login para Colaboradores distintos.

Todos os Colaboradores são orientados, inclusive através de normas internas, a desligarem seus equipamentos no final do dia, fazendo logoff de todos os sistemas, bem como a manter documentos físicos trancados. Qualquer documento mantido sobre a mesa dos Colaboradores ao final do dia é recolhido para guarda e devolução no dia útil seguinte.

Como forma de minimizar o risco de roubo de informações ou contaminações dos sistemas, não é permitida ou utilizada qualquer forma de acesso externo ou conexão com os servidores internos da MARR. A MARR adota, ainda, solução de Firewall de rede, antivírus Kaspersky e monitoramento da rede e do tráfego de dados, além de controlar eventuais instalações de sistemas ou softwares não autorizados, considerando que a MARR disponibiliza a todos os Colaboradores equipamentos e softwares licenciados, acesso à internet, bem como materiais e suporte necessário, com o exclusivo objetivo de possibilitar a execução de todas as atividades inerentes aos negócios da MARR.

7. SEGREGAÇÃO EM RELAÇÃO ÀS DEMAIS EMPRESAS NAS QUAIS OS SÓCIOS TENHAM PARTICIPAÇÃO SOCIETÁRIA

Os sócios e diretores da MARR poderão deter participações societárias em outros negócios.

Nesse sentido, com o intuito de segregar a atividade de gestão de recursos e evitar qualquer compartilhamento de informação, a MARR Gestão de Recursos determina que os sócios que possuam participação societária em outras empresas atuantes no mercado financeiro e de capitais não poderão ter atuação funcional em tal empresa, devendo figurar apenas como sócios de capital.

8. SISTEMA DE CONTROLES INTERNOS

A Diretoria de Riscos e Compliance, mantém disponível, para todos os Colaboradores, todas as Políticas publicadas na Intranet. As mesmas devem ser sempre respeitadas, inclusive, com formalização dentro do Sistema de Controles Internos – SCO. O referido sistema auxilia no cumprimento da regulação e autorregulação em vigor. O mesmo está sob responsabilidade da área de Controles Internos – Compliance, que cria os monitoramentos, acompanha as respostas registradas pelos colaboradores da primeira e segunda linha de defesa, por meio dos relatórios extraídos: do sistema, de controles, monitoramentos, colaboradores, entre outros. Os pontos de monitoramentos existentes são baseados no mapeamento das atividades realizadas, nas Políticas e normativas vigentes e contemplam controles de:

- Independência nas Atividades de Riscos
- Trilha de Auditoria
- TI - Sistema de Arquivamento
- Termo de Confidencialidade
- Conflito de Interesses
- Conflito de Interesses - Linhas de Defesa
- Leitura das Políticas Atualizadas na Intranet

- Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades

Caso qualquer Colaborador identificar situações que possam configurar como passíveis de conflito de interesse, deverá submeter imediatamente sua ocorrência para análise do Diretor de Riscos e Compliance.

9. REVISÃO DESTA POLÍTICA

O Diretor de Compliance deverá realizar uma revisão da política da segurança e sigilo da informação a cada 12 (doze) meses, no mínimo, para avaliar a eficácia da sua implantação.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes comas operações comerciais da MARR e acontecimentos regulatórios relevantes.